Washington University Journal of Law & Policy

Volume 14 *Justice, Ethics, and Interdisciplinary Teaching and Practice | Mental Health and the Law*

January 2004

The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring

Waseem Karim
Washington University School of Law

The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring

Waseem Karim*

I. INTRODUCTION

The United States Department of Defense designed the Global Positioning System (GPS) in the early 1970s to track the position of military troops and equipment.[1] GPS consists of a network of satellites that transmit radio signals to Earth, where a radio receiver then triangulates its own position based upon the readings from the satellites.[2] Following an airline mishap in the 1980s, GPS became available for civilian use and safety purposes due to its superior navigation capability.[3]

Since that time, civilian uses for GPS have expanded beyond aviation.[4] Because the receivers are relatively inexpensive,[5] GPS is used in a variety of capacities, such as car navigation, mineral and

---

* J.D. Candidate, 2004, Washington University School of Law.

1. ALESSANDRA A.L. ANDRADE, THE GLOBAL NAVIGATION SATELLITE SYSTEM: NAVIGATING INTO THE NEW MILLENNIUM 37 (2001). GPS made its "wartime debut" during the Persian Gulf War. SCOTT PACE ET AL., THE GLOBAL POSITIONING SYSTEM 1 (1996). GPS technology helped to guide missiles to hit precise targets. Brandon Eric Ehrhart, Note, *A Technological Dream Turned Legal Nightmare: Potential Liability of the United States Under the Federal Tort Claims Act for Operating the Global Positioning System*, 33 VAND. J. TRANSNAT'L L. 371, 378 (2000). For example, one may recall the image of a Standoff Land Attack Missile (SLAM), directed by GPS, blasting a hole in an Iraqi power plant, followed by a second SLAM that flew through the same hole. *Id*.

2. Aaron Renenger, Note, *Satellite Tracking and the Right to Privacy*, 53 HASTINGS L.J. 549, 550 (2002). Currently, the GPS consists of twenty-nine satellites. ANDRADE, *supra* note 1, at 24.

3. ANDRADE, *supra* note 1, at 38. Korean Airlines Flight 007 strayed off its course and was shot down when it flew into Soviet Airspace, prompting President Reagan to open GPS for civilian use free of charge. *Id*. at 38, 53 n.6.

4. *Id*. at 38.

5. *See* Ehrhart, *supra* note 1, at 375.

resource exploration, recreational activities such as camping, and weather forecasting.[6] Recently, the Federal Communications Commission (FCC) has required cellular phone providers to equip their phones with location-detecting capabilities.[7]

This Note will discuss the most novel use to date of GPS technology: the personal tracking device, or personal locator. Several companies have developed personal locators, which can pinpoint the exact location of the individual wearing the device. These personal locators are designed and intended for the average citizen to purchase and wear voluntarily. One might ask why the average citizen would want to wear a device that can pinpoint their location. Among the benefits of personal locators, as cited by their proprietors, is an ability to quickly identify the location of a person in an emergency medical situation.[8] However, the main reason that these devices have suddenly gained popularity is their ability to track the location of children.[9] As a result of a sudden increase in the media's coverage of child abduction cases, parents have experienced elevated fears of their own children's abduction.[10] For many parents, investing in a personal locator for their child is a reasonable precaution against abduction.[11]

Part II of this Note examines two personal locators that are currently on the market: Wherify Wireless's Personal Locator and Digital Angel. The section also examines the VeriChip, a microchip containing the personal information of the wearer, which is implanted under their skin.[12] Part II discusses the relationship between the heightened media coverage of child abductions during the summer of 2002[13] and the popularity of personal tracking devices.[14]

---

6. ANDRADE, *supra* note 1, at 38.

7. *See infra* notes 93-95 and accompanying text.

8. For more information, see Digital Angel's website, at http://www.digitalangel.net/consumer.asp (last visited Nov. 2, 2003).

9. *See, e.g.*, Benny Evangelista, *A High-Tech Eye on the Kid*, SAN FRANCISCO CHRONICLE, Aug. 19, 2002, at A1.

10. *Id.*

11. *Id.*

12. For more information, see VeriChip's website, at http://www.adsx.com/prodservpart/verichip.html (last visited Nov. 2, 2003).

13. *See, e.g.*, Evangelista, *supra* note 9.

14. *See, e.g.*, Hanna Kale Kinnersley, *Cranky Consumer: Tracking Kids By GPS*, WALL ST. J., Dec. 24, 2002, at D2 ("After this summer's high-profile child-abductions, parents are

Next, Part II discusses the privacy concerns raised by the use of these devices. Because the data generated from these devices could be valuable for a variety of purposes, including marketing research, this Note considers the level of privacy that a user of a personal tracking device can expect from unwanted access to their data. Furthermore, Part II considers the foreseeable use of these devices for government surveillance purposes. Although tracking devices have enormous potential for use in law enforcement, both in real-time tracking and in access to past location information, the potential for abuse is also extremely great. Part II discusses the manner in which courts have balanced the use of more primitive forms of tracking devices with the Fourth Amendment's protection against unreasonable search.[15] Part II also examines the government's ability to access data under the recently passed USA PATRIOT Act.[16]

Part III of this Note begins by speculating whether the sudden media coverage of child abductions in 2002 was intended to help to create a market for personal locators, particularly in light of both the corporate ownership of the media and the story selection process. Part III also discusses the inadequacy of both the current tort law and statutory privacy measures, as well as the problem of the "reasonable expectation of privacy" standard courts use in Fourth Amendment analysis. While some of the analysis may seem premature because of personal tracking devices' relatively recent development and currently limited market, personal use of location-detecting technology will undoubtedly expand as new benefits emerge and as the public becomes more accustomed to the notion. Thus, it is critical to be prepared for the legal problems that may arise. Furthermore, personal locators constitute merely one component in a larger progression towards surveillance and data monitoring.[17] With increased capabilities comes increased power, especially with regard

---

more concerned than ever about their children's safety.").

15. *See, e.g.*, United States v. Knotts, 460 U.S. 276 (1983).

16. Pub. L. No. 107-56, 115 Stat. 272 (2001).

17. *See* Jay Stanley & Barry Steinhardt, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society* (2003), *at* http://www.aclu.org/Privacy/Privacy.cfm ?ID=11573&c=39&Type=s#FileAttach (last visited Nov. 2, 2003) (discussing increased methods of data surveillance and the ability to link these technologies, resulting in a "surveillance monster").

to the government, and privacy law must be retooled in order to adequately protect against surveillance capabilities.[18]

Finally, Part IV of this Note proposes that the strongest protection of privacy from unwanted surveillance lies in the Fourth Amendment's protection against unreasonable search and seizure.[19] As the courts' current framework of analysis is inadequate in keeping up with the novel privacy concerns raised by new technology, a new focus of analysis should examine whether there is a "reasonable expectation of privacy" for the information once it is gathered.

II. THE EMERGENCE OF THE PERSONAL TRACKING DEVICE AND PRIVACY LAW AS IT STANDS

A. Personal Tracking Devices

This section will briefly examine the different personal tracking devices that have recently arrived on the market.

1. Wherify

Wherify Wireless, Inc.,[20] claims to have produced the first personal tracking device, called the Personal Locator.[21] Individuals can wear this device like a wristwatch, and Wherify is marketing it to parents for use in tracking their children.[22]

The Personal Locator uses both GPS technology and the Sprint PCS Network to pinpoint the location of the wearer. Parents can use

18. *Id.* at 14-17.

19. Originally limited to the protection of physical searches of personal property, the Fourth Amendment's protection was broadened to include electronic surveillance in the case of *Katz v. United States*, 389 U.S. 347 (1967). *See* Jennifer C. Evans, Comment, *Hijacking Civil Liberties: The USA PATRIOT ACT of 2001*, 33 LOY. U. CHI. L.J. 933, 943-47 (2002).

20. Timothy Neher founded the company in 1998. For more information, see Wherify's website, at http://www.wherifywireless.com/about_hist.htm (last visited Nov. 2, 2003).

21. *See* Wherify's website, *at* http://www.wherifywireless.com/prod_watches.htm (last visited Nov. 2, 2003).

22. *See* Doug Bedell, *Keeping a High Tech Watch on the Children*, THE RECORD, Sept. 15, 2002 (stating that Wherify is targeting the product towards children aged five to ten). The watch's cartoonish appearance also clearly indicates that Wherify is marketing its product to children. For a picture of the watches, see Wherify's website, at http://www.wherifywireless.com/prod_watches.htm (last visited Nov. 2, 2003).

the Internet to conduct a "locate" search to display an aerial map of the child's exact location.[23] Users can also employ a "Locate History" function that allows them to view thirty days worth of location data.[24] Parents can track the child's location at ten-minute intervals by using the "Bread Crumb" feature.[25] Because the Personal Locator employs the Sprint PCS system, a child can use the Personal Locator device to call 911,[26] and the device will automatically dial 911 if someone tries to cut it off or if the child wanders beyond the perimeter of a preset area.[27] Wherify has shipped 1,000 units since releasing its product in July 2001, and it has received close to 100,000 orders through its website.[28] Soon, retailers will begin to carry the Personal Locator.[29]

2. Digital Angel

Applied Digital Solutions (ADS), through its subsidiary Digital Angel Corp., has produced a wristwatch-style GPS device known as Digital Angel.[30] Using AT&T Wireless Services,[31] the device triggers a "WanderAlert" in the event that the wearer moves beyond the

23. See Wherify's website, at http://www.wherifywireless.com/prod_locserv.htm# (last visited Nov. 2, 2003), for a demonstration of the Wherify Internet system. At this website, one can perform a simulated "Locate," which gives an aerial photograph of Manhattan with the number "1" indicating the location of the simulated child. *Id.* The "Locate" function also gives a timestamp indicating when the child was at the location, the address of the child's location, and the longitudinal and latitudinal coordinates indicating the location. *Id.*

24. *See id.*, which also simulates the "location history" function. In this demonstration, there are four positional numbers with timestamps, addresses, and coordinates, indicating where the simulated child has traveled between 9:56 and 10:11 on the morning of January 23. *Id.*

25. *See* Bedell, *supra* note 22.

26. The Personal Locator uses the Sprint PCS system to monitor the child's 911 distress call. *Id.*

27. Elizabeth V. Mooney, *Wireless Moves Beyond Devices to Clothes, Skin Chips*, RCR WIRELESS NEWS, Sept. 2, 2002, at 13.

28. Evangelista, *supra* note 9.

29. *See* Doug Olenick, *Wherify Ships GPS Locator This Month*, TWICE, Sept. 2, 2002, *available at* http://www.twice.com/index.asp?layout=story&articleId=CA241868&pubdate=09/02/2002 (last visited Nov. 2, 2003) (stating that Wherify President Timothy Neher, though unable to say which retailers would "participate in the [products'] rollout," said that "it would be in the major consumer electronic chains").

30. *See* Mooney, *supra* note 27.

31. *Id.* The AT&T Network is used to relay the information from the GPS locator to Digital Angel's Operation Center. For an illustrated demonstration of the system, see Digital Angel's website, at http://www.digitalangel.net/works_demo.asp (last visited Nov. 2, 2003).

perimeter of a preset area.[32] Digital Angel does not boast the high number of orders that Wherify does; it has sold 200 units and has received orders for 1,000 more.[33]

3. VeriChip

Perhaps the most intriguing new device is the VeriChip.[34] The VeriChip is a miniaturized radio frequency identification device (RFID)—the size of a grain of rice—which stores a person's unique verification number, from which one can access his personal information, including medical information. What makes the VeriChip so unique is that it is surgically imbedded underneath a person's skin. A special scanner, when passed over the VeriChip, can read the chip's information.[35] Thus, a hospital equipped with a special scanner could obtain a patient's medical history by reading his VeriChip.[36] As of this writing, nine people have received

32. *See* Vincent J. Schodolski, *Parents Look to Technology to Track Kids*, CHICAGO TRIB., Sept. 9, 2002, at 1. For an illustrated demonstration on how the WanderAlert functions, see Digital Angel's website, at http://www.digitalangel. net/works_demo (last visited Nov. 2, 2003). The GPS monitor sends a message through AT&T's wireless service to a cellular tower when the wearer wanders beyond a preset boundary. *Id*. The monitor then relays the message to Digital Angel's operation center, which gives an alert to the designated caregiver. *Id*.

In addition to using GPS, the Digital Angel monitors the wearer's vital signs and changes in the environment. *See id*. The "ThermAlert" triggers an alert when there is a drastic change in the wearer's environmental surroundings. *Id.* "Such a shift could suggest that those prone to wandering have inadvertently encountered a potential harmful situation." *Id*. The Digital Angel can also send an alert when the wearer has fallen down. *Id*.

Monitoring vital signs and sending an alert if the wearer has fallen down indicates that one of the main purposes of the Digital Angel is to monitor senior citizens, particularly those afflicted with Alzheimer's Disease. Based on the information from the company's website, it appears as though Digital Angel is not marketing their products primary towards children, as Wherify is. Digital Angel representatives advertise that their product is designed for active senior citizens, impaired senior citizens, families on the go, and pets. *Id*.

33. *See* Mooney, *supra* note 27.

34. Applied Digital Solutions, who also manufactures Digital Angel, produces the VeriChip.

35. VeriChip's website states: "Utilizing an external scanner, radio frequency energy passes through the skin energizing the dormant VeriChip, which then emits a radio frequency signal containing the verification number. The number is displayed by the scanner and transmitted to a secure data storage site by authorized personnel via telephone or Internet." For more information, see the product's website, at http://www.adsx.com/prodservpart/verichip.html (last visited Nov. 2, 2003).

36. The Global VeriChip Subscriber registry service (GVS) provides access to the database containing the information of the individual with the implant. *Id.* Using a scanner,

VeriChip implants,[37] including the members of the Jacob family, who received a great deal of publicity when they were implanted with VeriChip live on NBC's Today Show.[38] In addition to medical uses, the company is promoting the device's use for security purposes,[39] such as controlling access to secure areas and functioning as a personal verification system to prevent identity theft.[40] While the VeriChip does not currently have GPS technology, in May 2003, ADS successfully tested a working prototype of an implantable GPS device.[41]

Currently, there are twelve centers authorized to implant VeriChips in eight different states.[42] ADS also has agreements to distribute VeriChip in Mexico, Russia, Columbia, and Venezuela.[43] Like a soft-drink company sending promotional buses to ballgames

---

healthcare providers could access the GVS to retrieve medical information such as preexisting medical conditions and emergency contact numbers. *Id*.

37. Lini S. Kadaba, *Taking a High-Tech Approach to Child Security*, PHILADELPHIA INQUIRER, Aug. 15, 2002.

38. Glenn Singer, *ID Chip Debuts; Stock Plummets; Applied Digital Media Blitz Fails to Allay Concerns*, S. FLA. SUN-SENTINEL, May 11, 2002, at 12B. The scanners will sell for $1,000-$1,500. Beatrice E. Garcia, *First Chip Implant Procedures Go Without Hitch*, MIAMI HERALD, May 11, 2002.

39. *See* VeriChip's website, *supra* note 35.

40. *Id*. The company explains that both government facilities and privately owned buildings can use the device. *Id*. VeriChip's use as a personal verification system is an "enormous, untapped potential," according to the company, citing its ability to secure access to banking and credit card accounts. *Id*.

The British government's Home Office is debating yet another use for an implantable GPS tracking device. Dominic Tonner, *Pedophiles May Be Fitted with Electronic Tags*, SUNDAY TIMES – LONDON, Nov. 17, 2002, at 5. The government is considering a plan to implant convicted pedophiles with GPS tracking devices. *Id*.

41. Laureen Fagan, *Is the Price Right? Some Believe Bids for National Security Come at the Cost of Americans' Civil Liberties*, S. BEND TRIB., May 18, 2003. In England, Kevin Warwick, a professor at Reading University, is developing a GPS microchip of his own that can be implanted into a person. Sally Weale, *Parents—Would You Microchip Your Child?*, GUARDIAN, Sept. 4, 2002, at P8; *see also* Margarett Driscoll, *This Girl's Parents Want to Keep Track of Her by Microchip: Paranoia or Wise Precaution?*, SUNDAY TIMES – LONDON, Sept. 8, 2002, at 24. Eleven-year-old Danielle Duval is ready to receive the first microchip implant. Driscoll, *supra*, at 24.

42. On October 22, 2002, the Food and Drug Administration announced that the VeriChip is not a regulated medical device for safety, financial, and personal identification/safety applications, but rather is a regulated medical device when marketed "to provide information to assist in the diagnosis or treatment of injury or illness." *FDA Rules on Applied Digital's Chip*, S. FLA. SUN-SENTINAL, Oct. 23, 2002, at 1D.

43. BUSINESS WIRE, July 23, 2003.

and college campuses, the company has a "ChipMobile" that travels to popular areas to promote the VeriChip.[44]

B. The Media's Influence on Public Perception

The proliferation of personal tracking devices depends upon the public's willingness to purchase and voluntarily use these devices. As discussed above, parents' desires to protect children from potential kidnappers have contributed to the demand for the locators[45] and has been a selling point for their proprietors.[46]

Beginning in the summer of 2002, the media focused heavily on coverage of child abduction cases.[47] This coverage, in turn, prompted reports on the fact that media coverage itself had increased.[48] Statistically, however, the number of child abductions has *decreased* over the past several years.[49] Despite this actual decrease in child abductions, however, the media coverage has heightened fears of abduction, precipitating interest in personal locators.[50]

1. Media Ownership

Because of the sudden, and seemingly unprovoked, media attention towards child kidnappings, we must ask: why the sudden media interest? An answer to this question may be discovered in the structure of media ownership, and the decision-making process involved in reporting.

---

44. See Verichip's website, *supra* note 35.

45. *See, e.g.*, Evangelista, *supra* note 9.

46. *See, e.g.*, Bedell, *supra* note 22 and accompanying text (describing Wherify's efforts to market their product for children).

47. *See, e.g.*, Kadaba, *supra* note 37; *see also* Evangelista, *supra* note 9. The media in England also began emphasizing child abductions. *See, e.g.*, Driscoll, *supra* note 41 ("Having your child surgically implanted with a microchip may be extreme, but the killings of Holly Wells, Jessica Chapman and Sarah Payne . . . have stirred parental fears to unprecedented levels.").

48. *See, e.g.*, Stephanie Dunnewind, *Parent Panic; It's Just Human Nature, Say Psychologists, That Makes Parents fear Child Abductions out of Proportion with Reality*, SEATTLE TIMES, Sept. 10, 2002, at E1.

49. *See, e.g.*, Evangelista, *supra* note 9.

50. Evangelista writes, "With stories about missing and abducted children . . . seemingly making headlines every week, Wherify and makers of similar tracking devices . . . are receiving an increasing number of calls from consumers and the media." *Id.*

Recently, mergers and acquisitions have increasingly consolidated American media.[51] Critics argue that this concentration of media ownership in a handful of corporations can have a stifling effect on the free exchange of information,[52] which results from the corporate ownership's manipulation of the content.[53] The potential influence of media ownership on the marketplace for personal tracking devices is analyzed later in this Note.[54]

Another influence on story selection is the tendency to report on information that is already circulating.[55] Due to deadlines and other constraints, it is difficult for reporters to seek novel stories about which to report.[56] As a result, there is a "media frenzy," where various news organizations give one particular issue substantial attention, all relying upon the same source of information.[57]

---

51. *See generally* Donald R. Simon, Comment, *Big Media: Its Effect on the Marketplace of Ideas and How to Slow the Urge to Merge*, 20 J. MARSHALL J. COMPUTER & INFO. L. 247 (2002). Some of the most prominent media mergers include Disney and Capital Cities/ABC, Viacom and CBS, and America Online and Time-Warner. *Id.* at 248. Most recently, on June 2, 2003, the FCC approved a measure to relax media ownership restrictions by a 3-2 vote. *See, e.g.*, Yochi J. Dreazen & Joe Flint, *FCC Eases Media-Ownership Caps, Clearing the Way for New Mergers*, WALL ST. J., June 3, 2002, at A1. The two dissenters, Commissioners Adelstein and Copps, were sharply critical of the decision and warned that a small number of companies would have too much influence over the media. *Id.*

52. As ownership concentrates, access to the media also narrows to exclude those with viewpoints that do not fit within the permissible range of discussion. Anne Benaroya, Note, Philadelphia Newspapers v. Hepps *Revisited: A Critical Approach to Different Standards of Protection for Media and Nonmedia Defendants in Private Plaintiff Defamation Cases*, 58 GEO. WASH. L. REV. 1268, 1288 (1990). *See also* Paul Wellstone, *Growing Media Consolidation Must Be Examined to Preserve Our Democracy*, 52 FED. COMM. L.J. 551, 552 (2000) ("[O]ne corporate conglomerate can still exercise control over the content of media that reaches citizens through many different outlets. The safest and best way to ensure diversity of viewpoint is through diverse ownership.").

53. Wellstone, *supra* note 52, *passim*. The Columbia Journalism Review and the Pew Center for the People and the Press conducted a survey that revealed that 61% of journalists feel that parent corporations have influence on story selection. *Id.*

54. *See infra* notes 138-___ and accompanying text.

55. CARLA BROOKS JOHNSTON, SCREENED OUT: HOW THE MEDIA CONTROL US AND WHAT WE CAN DO ABOUT IT 123 (2000).

56. *Id.*

57. Sarah Eschholz, *The Media and Fear of Crime: A Survey of the Research*, 9 U. FLA. J.L. & PUB. POL'Y 37, 47-48 (1997).

2. Fear and the Media

Commentators charge that the media encourages the public to remain in a state of panic and apprehension about every danger that may exist.[58] They argue that society has become increasingly preoccupied with risks, threats, and safety.[59] Whether the media is the chief cause of society's state of anxiety[60] or simply amplifies a preexisting sense of risk and fear,[61] the media stays true to the saying "if it bleeds, it leads," by using violence and fear to increase its ratings.[62] Viewers will feel the need to consume more news in order to stay up-to-date on the latest harms.[63] When individuals feel vulnerable, they are willing and open to accept an offered solution to alleviate that fear.[64]

While the number of children kidnapped has not increased,[65] people have in recent years repeatedly heard about and seen the latest child abduction. Parents will naturally fear these stories that appear far more real than statistics, which are too abstract to grasp.[66] Through continuous repetition, the problem becomes a priority in the

58. *See generally* FRANK FUREDI, CULTURE OF FEAR (Continuum 2d ed. 2002) (1997).

59. *Id.*

60. JOHNSTON, *supra* note 55, at 8. Johnston points to the "Y2K" scare over the millennium computer bug, and writes that the public would not have been stirred into a frenzy had they not heard about it from the media. *Id*.

61. FUREDI, *supra* note 58, at 52-53. Furedi explains that, while the media plays a significant role in shaping the public's perception of risks, it is not the cause of society's sense of risk. *Id.* at 53.

62. Symposium, *Crime, Recidivism, Public Perception and the Media*, 23 S. ILL. U. L.J. 297, 306 (1999).

63. JOHNSTON, *supra* note 55, at 79.

64. *See id*. at 86. Anthony Pratkanis and Elliott Aronson state:

A fear appeal is most effective when:

- It scares the hell out of people.
- It offers a specific recommendation for overcoming the fear-arousing threat.
- The recommended action is perceived as effective for reducing the threat.

Id.

65. *See* Evangelista, *supra* note 9

66. Dunnewind, *supra* note 48. Kidnapping is the greatest fear for parents of children, from toddlers to teenagers. *Id.*

public mind, creating a sense of urgency about the threat of child abductions.[67]

C. Privacy Implications and the Protection of Personal Information

Considering the speed at which personal tracking devices are developing and the devices' perceived popularity,[68] they will soon proliferate. Furthermore, it is only a matter of time until the market sees a GPS device that will be surgically imbedded into a person, as ADS continues to make breakthroughs in technology.[69] As such, it is important to address the privacy concerns that the use of these devices raises. Moreover, these privacy concerns are not exclusive to personal tracking devices, as one can apply them to various new kinds of technology.[70] Personal locators have the ability to generate virtually limitless amounts of data about an individual.[71] For example, locations where the individual travels, shops, and eats are just a few of the many pieces of information that the proprietors of the devices can collect and relay to a wide variety of interested third parties.[72] Intimate details about an individual's life become available, and when these data are compiled, they create a comprehensive profile of a person.[73] Indeed, there are profiling companies devoted to aggregating data and selling profiles on individuals.[74] Obviously, this

67. BEN H. BAGDIKIAN, THE MEDIA MONOPOLY 16 (5th ed. 1997). Bagdikian explains, "It is in that power [of repetition]—to treat some subjects briefly and obscurely but others repetitively and in depth, or to take initiatives unrelated to external events—where ownership interests most effectively influence the news." *Id.*

68. *See, e.g.*, Evangelista, *supra* note 9.

69. *See supra* note 41 and accompanying text.

70. For a description of other kinds of technologies that implicate privacy, see *infra* note 155.

71. *See* Renenger, *supra* note 2 (exploring the possible ways in which marketers could use data collected from cell phones equipped with GPS technology).

72. Marketers, however, are not the only third parties that could be interested in this data. James Dempsey of the Center for Democracy and Technology explains, "[W]hat if your insurer finds out you're into rock climbing or late-night carousing in the red-light district? What if your employer knows you're being treated for AIDS at a local clinic? The potential is there for inferences to be drawn about you based on knowledge of your whereabouts." *Id.* at 563 (quoting Simon Romero, *Location Devices' Use Rises, Prompting Privacy Concerns*, N.Y. TIMES, Mar. 4, 2001, at 1).

73. Stanley & Steinhardt, *supra* note 17, at 11-12.

74. Data is collected on a wide range of information, drawing on everything from book preference to lactose intolerance. See the Electronic Privacy Information Center's Privacy and

information is extremely valuable.[75] Therefore, it is important to consider what rights people who voluntarily wear personal locators have to protect their personal information from third parties.

1. Privacy rights in tort law

The Second Restatement of Torts recognizes four privacy torts.[76] For the purposes of tracking devices, Section 652A(1)(A) and (1)(B)—the torts for unreasonable intrusion upon the seclusion of another and for dissemination of an individual's private information—are applicable.[77]

If an individual wearing a personal locator whose information was sold to a third party were to seek a claim due to publicity dispersed regarding his private life, he must show that the matter publicized was of a kind that would be "highly offensive to a reasonable person," and that the information was "not of legitimate concern to

---

Consumer Profiling webpage, at http://www.epic.org/privacy/profiling/ (last visited Nov. 2, 2003) for a list of the kinds of data gathered. Profiles are indexed in a variety of different ways. *Id.* The American List Counsel, for example, sells an "ultra affluent database." *Id.*

75. In fact, consumer information that is not collected is considered to be "money left on the table." Stanley & Steinhardt, *supra* note 17, at 4.

76. The Second Restatement of Torts states:

> (1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.
>
> (2) The right of privacy is invaded by
>
> (a) unreasonable intrusion upon the seclusion of another . . . or
>
> (b) appropriation of the other's name or likeness . . . or
>
> (c) unreasonable publicity given to the other's private life . . . or
>
> (d) publicity that unreasonably places the other in a false light before the public . . . .

RESTATEMENT (SECOND) OF TORTS § 652A (1977).

77. The "false light" privacy tort is inapplicable because the commercial use of personal information does not concern whether the information is false, but rather whether it can be made public. Renenger, *supra* note 2, at 556. The misappropriation tort, which applies to the misuse of an individual's name or image, is also inapplicable because the individual's name or image is not likely to be the matter of concern. *Id*. *See also* Richard C. Balough, *Global Positioning System and the Internet: A Combination with Privacy Risks*, 15 CBA REC. 28, 29-32 (2001).

the public."[78] However, under this tort, a person cannot recover damages when he is in the public eye, as the intrusion does not pertain to his private life.[79]

For liability to exist under the intentional intrusion of privacy tort, there must be an "intentional intrusion upon the solitude or seclusion of another," and the intrusion must be of a kind that is "highly offensive to a reasonable person."[80] Because the tort involves an individual's solitude, liability generally does not exist when the individual is in the public eye.[81] However, solitude is not dependant upon whether the location is private, but rather upon the expectation of privacy and the kind of invasion that takes place.[82]

---

78. Renenger, *supra* note 2, at 556-57 (citing RESTATEMENT (SECOND) OF TORTS § 652D (1977)). The Restatement provides several illustrations to define what would be highly offensive to a reasonable man:

> 9. When A's daughter is married, A holds in his home a private wedding, to which only members of the family and a few intimate friends are invited. B Newspaper obtains information from those present and publishes an accurate account and description of the wedding. This is not an invasion of the privacy of A.
>
> . . . .
>
> 11. A is about to give birth to a child, and is told that a caesarian operation will be necessary. She agrees to allow B to make a motion picture of the operation for exhibition to medical students for educational purposes. B exhibits the picture to the public in a commercial theater. This is an invasion of A's privacy.

RESTATEMENT (SECOND) OF TORTS § 652D cmt. c, illus. 9, 11 (1977).

79. *Id.*

80. *Id.* § 652B. Whether the information is publicized is irrelevant for this tort, as liability depends solely upon whether the individual's solitude was intruded upon. *Id.* § 652B cmt. a.

81. *Id.* § 652B cmt. c.

82. *Id.* The Restatement explains, "[T]here is no liability for the examination of a public record concerning the plaintiff." *Id.* However, the Restatement also states that there can be liability, even in public areas, when there exists an expectation of privacy. *See id. See also* Evans v. Detlefsen, 857 F.2d 330, 338 (6th Cir. 1988) (holding that the location of the intrusion is relevant in helping to determine the sufficiency of evidence of seclusion, but is not outcome determinative, as seclusion is defined by the type of interest involved). Some courts have interpreted the case law to mean the plaintiff must show an actual, subjective expectation of seclusion and that this expectation was objectively reasonable. *See* Med. Lab. Mgmt. Consultants v. Am. Broad. Cos., Inc., 306 F.3d 806, 812-13 (9th Cir. 2002). Others have found that an intrusion occurs when the actor is substantially certain that he lacks permission to commit an intrusive act. *See* Fletcher v. Price Chopper Foods of Trumann, Inc., 220 F.3d 871, 876 (8th Cir. 2000).

2. FCC regulation of GPS in cellular phones

The privacy concerns regarding the commercial use of customer data that will foreseeably arise with the use of personal tracking devices can be evaluated by a comparison to a similar debate involving customer data collected by telecommunications carriers, especially in light of the availability of location-detecting technology in cellular phones.[83]

Because telecommunications carriers have the capacity to collect vast amounts of data from an individual using their service, Congress took measures to protect information collected from consumers, involving Customer Proprietary Network Information (CPNI).[84] When it passed the Telecommunications Act of 1996, Congress included section 222, which requires telecommunications companies to obtain customer approval before distributing CPNI to third parties.[85]

A controversy arose because the Act did not clarify the manner in which the companies could obtain customer approval.[86] The FCC created a regulation[87] adopting an "opt in" approach that requires a telecommunications carrier to obtain express customer consent to market CPNI to third parties.[88] Telecommunications carrier U.S.

83. *See infra* note 95 and accompanying text.

84. Ellen Traupman, *Who Knows Where You Are? Privacy and Wireless Services*, 10 COMM. LAW CONSPECTUS 133, 134 (2001). CPNI includes "virtually all information about a customer's use of network services that a [carrier] may acquire in providing those services." *Id.* at 137 (quoting PETER H. HUBER ET AL., FEDERAL TELECOMMUNICATIONS LAW 1257 n.235 (1999)).

85. *Id*. at 139 (citing 47 U.S.C. § 222(c)(1) (1996)). The Act, in relevant part, reads:

> [A] telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

47 U.S.C. § 222(c)(1) (2003).

86. *See* Traupman, *supra* note 84, at 139.

87. 13 FCC Rec. 8061 (1998).

88. *See* Traupman, *supra* note 84, at 139. *See also* Brian A. Kelley, Note, U.S. West, Inc. v. FCC: *Exposing the Deficiencies in Government Attempts to Protect Customer Privacy*, 52 ADMIN. L. REV. 1055, 1056 n.8 (quoting the FCC regulation that codifies the CPNI order). "A telecommunications carrier must obtain customer approval to use, disclose, or permit access to

West challenged the FCC's interpretation of section 222 in *U.S. West, Inc. v. FCC*.[89] In this case, the Tenth Circuit Court of Appeals found that the "opt-in" approach constituted an undue restriction on commercial speech protected by the First Amendment.[90] In July 2002, the FCC issued the Final CPNI Order,[91] which is current to date, allowing telecommunications carriers to use an "opt-out" approach when sharing CPNI with affiliate companies, but still requiring an "opt-in" procedure when sharing information with third parties.[92]

Under the Wireless Communications and Public Safety Act of 1999 (WCPSA), Congress authorized the FCC to administer the deployment of enhanced wireless 911 (E-911) services.[93] The FCC established a regulation[94] that requires cellular phone companies to include location-detecting technology in their cellular phones in order to track the originating location of 911 calls.[95]

CPNI to market to a customer service to which the customer does not already subscribe to from that carrier." 47 C.F.R. § 64.2005(b)(1)-(2).

89. 182 F.3d 1224 (10th Cir. 1999).

90. *Id*. at 1240. The court found that a restriction on the audience of speech is a restriction on the speech itself. *Id*. at 1232. Addressing the issue of customer privacy, the court explained that the government failed to show that releasing CPNI would cause specific and significant harm to customers. *Id.* at 1235. The court found that a general level of discomfort in knowing that personal information is circulating does not rise to the level of a substantial state interest, explaining that "we live in an open society where information may usually pass freely." *Id*.

In a dissenting opinion, Judge Briscoe wrote that the CPNI Order does not directly impact the carrier's expressive activity. *Id.* at 1243. Rather, it narrowly impacts the telecommunication companies' non-expressive speech by requiring them to obtain, rather than imply, consent. *Id*. at 1243-44. As such, this limited impact does not warrant First Amendment scrutiny. *Id*. at 1244. The dissent explained that it was not the job of the FCC to provide a justification for the privacy interest. *Id*. at 1245. Rather, the FCC was merely carrying out the privacy interest that Congress already articulated in section 222. *Id*.

91. 17 FCC Rec. 14,860 (2002).

92. Chris Jay Hoofnagle, *Consumer Privacy in the E-Commerce Marketplace*, INTERNET L. & BUS., Aug. 2002, at n.99 and accompanying text, a*vailable at* http://www.epic.org/epic/staff/hoofnagle/ilbpaper.html (last visited Nov. 2, 2003).

93. Pub. L. No. 106-81, 113 Stat. 1286 (1999) (codified as amended at 47 U.S.C. § 615 (2003)).

94. 47 C.F.R. § 20.18 (2002).

95. *See* Traupman, *supra* note 84, at 134. The regulation states, "Licensees . . . must provide to the designated Public Safety Answering Point Phase II enhanced 911 service, *i.e.*, the location of all 911 calls by longitude and latitude . . . ." 47 C.F.R. § 20.18(e) (2002).

Telecommunications providers were generally required to implement this regulation by October 1, 2002. 47 C.F.R. § 20.18(d) (2002). However, the FCC has extended the deadlines because telecommunications providers were falling behind schedule. John Dorschner, *Location*

As a result of the location-detecting capability of cellular phones, Congress amended the definition of CPNI to include location information.[96] The WCPSA requires a customer's "express prior authorization" before location information may be disclosed.[97] This language also caused controversy because the Act does not explain the procedure for gaining customer authorization.[98] Despite this ambiguity, it is clear that authorization cannot be implied, and it appears as though a customer must "opt-in" before a telecommunications carrier may disclose location information.[99]

The recent debate over the manner in which to regulate telecommunication carriers' use of CPNI and location information is useful in predicting and evaluating some of the issues that will arise from personal tracking devices. While a personal locator is subject to FCC regulation,[100] it is likely that these devices do not fall under the current regulations applicable to telecommunications carriers.[101]

Still Hard to Pinpoint by Cellphone, MIAMI HERALD, June 2, 2002. The deadline for full deployment is December, 2005. *Id*.

Telecommunications companies have the option to use either network-based technology to provide location information, or to incorporate GPS technology into cell phones. Renenger, *supra* note 2, at 551-52. Sprint PCS, Alltel, and Nextel are using GPS technology. *Id.* at 552.

Telecommunications carriers are developing E-911 to combine with advanced mapping systems that can not only plot the location of a call, but also detail crime statistics, report traffic jams, and report other events occurring in the area. David J. Phillips, *Beyond Privacy: Confronting Locational Surveillance in Wireless Communcation*, 8 COMM. L. & POL'Y 1, 5 (2003).

96. *See* 113 Stat. 1286.

97. 47 U.S.C. § 222(f) (2002).

98. *See* Traupman, *supra* note 84, at 144.

99. *Id.* The FCC denied a request from the Cellular Telecommunications and Internet Association (CITA) to clarify their position regarding the distribution of location information, as they expressed that Congress's intent was sufficiently clear. *See id.* Privacy advocates nevertheless worry that, without specific FCC guidelines addressing location information, the telecommunications carriers have too much flexibility to adopt their own approaches. *Id.* Telecommunications carriers are also upset with the FCC's refusal to clarify their position because it leaves them in a position of uncertainty. E-mail from Chris Hoofnagle, Associate Director, Electronic Privacy Information Center, to Waseem Karim (Feb. 12, 2003, 14:56 CST) (on file with the Washington University Journal of Law & Policy).

100. The ability to regulate these devices falls under the FCC's umbrella. *See* 47 U.S.C. § 151 (2001) (creating the FCC's power to regulate communication by radio). *See also* 47 U.S.C. § 153(43) (2001) (defining "telecommunications" to mean "the transmission, between or among points specified by the user, of information of the user's choosing without change in the form or content of the information sent and received"); 47 U.S.C. § 153(44) (2001) (defining "telecommunications carrier" to mean "any provider of telecommunications services").

101. In an e-mail to the author, a representative from the FCC, while speaking only from

D. Government Data Collection and Surveillance

Up to this point, this Note has considered privacy concerns relating to the consumer data generated by personal tracking devices. However, another potential privacy problem involves the government's possible use of the devices for surveillance and data collection. Given the enormous potential that these devices can have for law enforcement, it is certainly conceivable that law enforcement officials will attempt to use them. Recently, for example, police departments have used GPS systems in automobiles to track carjacking suspects.[102] As history has shown, the government has tried to use surveillance—legally or illegally—when opportunities to do so are available, and a greater opportunity than the personal locator for the surveillance of people is scarcely imaginable.[103] As such, we must consider the degree to which people who use GPS tracking devices are making themselves vulnerable to surveillance and profiling.

Where corporations have the potential to collect data about individuals for their use, the government has the capability to consolidate the information and to create all-inclusive profiles on individuals.[104] While the Privacy Act of 1974[105] prohibits the

---

personal opinion, explained that personal locator companies must register their equipment with the FCC in the same manner that the manufacturers remote control garage door opener must. E-mail from FCC Consumer Center, to Waseem Karim (Oct. 23, 2002, 09:09 CST) (on file with the Washington University Journal of Law & Policy). Therefore, registration alone does not make a personal locator proprietor a telecommunications carrier. Furthermore, it was the representative's opinion that personal locator companies are not considered to be telecommunications carriers. *Id.*

102. In July 2003, cars stolen in various U.S. cities were tracked via GPS systems. *See, e.g.*, Mike Musgrove, *Guardian Angels of the Highway*, WASH. POST, July 20, 2003 at F07.

103. *See* Mark G. Young, Note, *What Big Eyes and Ears You Have!: A New Regime for Covert Government Surveillance*, 70 FORDHAM L. REV. 1017, 1076-77 (2001) (discussing congressional discoveries revealing the FBI's practice of illegally wiretapping political figures and dissidents in the late 1960s and early 1970s).

Illustrating an example of police abuse, the ACLU cites an instance from 1997 in which a top ranking Washington, D.C. official used the police database to blackmail married individuals who frequented gay clubs. ACLU, *What's Wrong with Public Video Surveillance?* (undated) (on file with the Washington University Journal of Law & Policy). Should law enforcement have the capacity to gain location information about an individual twenty-four hours-a-day, the potential for abuse would also be enormous.

104. Stanley & Steinhardt, *supra* note 17, at 7-8.

105. 5 U.S.C. § 552a (1996).

government from maintaining profiles on individuals who are not the targets of investigation,[106] the Act does not prohibit the government from purchasing information from private organizations.[107] In fact, reports indicate that the Justice Department has an eight million dollar contract with Choicepoint, a data collection company, for access to their database of personal information.[108]

1. The history of tracking device and technological surveillance

The GPS-equipped personal locator is a recent technology. However, the tracking device itself is not a new concept, and law enforcement has been using various forms of location-detecting devices for years.[109] Consequently, there is judicial precedent regarding the use of tracking devices.

In *United States v. Knotts*,[110] law enforcement officials placed a "beeper" (radio transmitter) on a chloroform container that the defendant had purchased.[111] The police followed the defendant's automobile to his cabin, which was a drug laboratory, and, naturally, they arrested him.[112] The Eighth Circuit Court of Appeals reversed the conviction on the grounds that the use of the beeper was an unreasonable search and seizure under the Fourth Amendment.[113] Relying on *Katz v. United States*,[114] the Supreme Court reversed the Eight Circuit, holding that there was no Fourth Amendment violation

106. Stanley & Steinhardt, *supra* note 17, at 8.

107. *Id. See also* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 583 n.170 (1995) (stating that the Act does not affect the ability of agencies to obtain personal information from private organizations).

108. Stanley & Steinhardt, *supra* note 17, at 8. EPIC obtained documents under the Freedom of Information Act revealing the extent to which United States government agencies have contracts with ChoicePoint to obtain information about both U.S. and foreign citizens. The documents are available at http://www.epic.org/privacy/publicrecords/inschoicepoint.pdf, and http://www.epic.org/privacy/publicrecords/citizenprices.pdf.

109. *See generally* Clifford S. Fishman, *Electronic Tracking Devices and the Fourth Amendment:* Knotts, Karo, *and the Questions Still Unanswered*, 34 CATH. U. L. REV. 277 (1985).

110. 460 U.S. 276 (1983).

111. *Id.* at 278.

112. *Id*. at 278-79.

113. *Id*. at 279.

114. 389 U.S. 347 (1967).

because the defendant could not reasonably expect privacy when he was traveling in an automobile on public roads.[115]

The Washington State Court of Appeals considered the use of the more sophisticated GPS locator in *State v. Jackson*.[116] This case involved a missing child, the father of whom was the prime suspect.[117] The police obtained a warrant[118] to place GPS tracking devices on the father's automobiles.[119] Via the GPS monitor, investigators were able to track the father to a location where the child's missing body was found.[120] The appellant argued that the trial court erred in upholding the search warrants.[121] The State contended that search warrants were unnecessary because there was no requirement to show probable cause to place the GPS tracking device.[122] The *Jackson* court relied on the Washington State Constitution, using the "private affairs" inquiry, a broader test than the Fourth Amendment's "subjective and reasonable expectation of

115. *Knotts*, 460 U.S. at 281-82. The Court relies on two questions raised in *Katz*, asking whether the defendant exhibited a subjective expectation of privacy and whether the subjective expectation of privacy was one that society would recognize as reasonable. *Id.* at 281-82.

Furthermore, the Court found that the use of devices that heighten an individual's sensory perception, such as binoculars for seeing, are not prohibited, so long as the subject is available in some manner to the public. *Id*. at 282.

As an interesting aside, the defendant argued that should the government prevail, then "twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision." *Id*. at 283 (quoting the defendant's brief). The Court responded, "[I]f such dragnet-type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Id*. at 284.

United States v. Karo, 468 U.S. 705 (1984), also involved a situation in which law enforcement officials placed a beeper on a container of chemicals to track the defendant's movement. *Id.* at 708-10. The Court held that it was not a search for law enforcement officials to place the beeper on the container unbeknownst to the defendant. *Id*. at 713. However, the Court afforded Fourth Amendment protection when the beeper was no longer in a public location and moved to a private location. *Id*. at 714. *See also* Fishman, *supra* note 109, at 280.

116. 46 P.3d 257 (Wash. Ct. App. 2002).

117. *Id*. at 260-61.

118. In *Knotts*, the police did not have a warrant to place the beeper on the can of chloroform. In addition to examining the validity of the search warrants, the court in *Jackson* also examined the same issue that arose in *Knotts*: whether a probable cause obligation necessitating a warrant even exists under the circumstances. *Id*. at 268.

119. *Id*. at 261.

120. *Id*. at 261-62.

121. *Id*. at 268.

122. *Id*.

privacy" standard articulated in *Katz*.[123] Nevertheless, the court determined that when something is available to the public eye, the court will not consider it to be a person's private affair.[124]

In *Kyllo v. United States*,[125] the United States Supreme Court considered whether the use of a thermal imaging detector constituted an unreasonable search under the Fourth Amendment.[126] Here, the police scanned Kyllo's home with a thermal imaging device[127] to detect the levels of heat emanating from different areas of the home; the police then matched the heat's consistency with that of high-intensity lamps used for marijuana growth.[128] The Court found the use of the device to be an unreasonable search under the Fourth Amendment,[129] and determined that a minimal and reasonable expectation of privacy exists in the home.[130] Considering the use of sense-enhancing technology, the Court held that a search occurs when technology obtains information "that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,'" and the technology used "is not in general public use."[131]

---

123. *Id*. at 269. The court relied on Article I, section 7 of the Washington Constitution, which states, "No person shall be disturbed in his private affairs, or his home invaded, without the authority of law." *Id*. at 268 (quoting WA CONST. art. I, § 7).

124. *Id*.

125. 533 U.S. 27 (2001).

126. *Id*. at 29.

127. *Id.* Developed by the United States Army, thermal imagers can detect the infrared radiation from an object and produce a visual image. Amy Miller, Note, Kyllo v. United States: *New Law Enforcement Technologies and the Fourth Amendment*, 51 U. KAN. L. REV. 181, 185 (2002).

128. *Kyllo*, 533 U.S. at 29-30.

129. *Id*. at 40-41.

130. *Id*. at 34.

131. *Id.* (internal citation omitted). The Court articulated that it did not want to "leave the homeowner at the mercy of advancing technology." *Id.* at 35.

Arguing that the use of thermal detectors was not a search, the dissenting opinion explained that there is no reasonable expectation of privacy from heat waves that emanate from a building. *Id*. at 43-44 (Stevens, J., dissenting). In addition, the dissent criticized the criterion that the use of a technology can amount to a search if it "is not in general public use," charging that the requirement is "somewhat perverse" because "the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available." *Id.* at 47 (Stevens, J., dissenting).

2. Surveillance legislation

Practically speaking, law enforcement officials could obtain the data from personal tracking devices with relative ease. This point is especially clear when one considers the fact that the Department of Defense operates the GPS.[132] As such, the question is whether law enforcement can access the data *legally*.

Legislation pertaining to electronic surveillance has been modified repeatedly over the years,[133] the most recent development of which has been the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, or the USA PATRIOT Act.[134] Generally, this legislation broadens federal law enforcement's authority to use surveillance and eliminates barriers in retrieving intelligence information.[135] In particular, by lowering the standard of proof and reducing judicial oversight, the Act broadens the FBI's ability to obtain the information that a business maintains about an individual when the FBI is conducting an intelligence investigation.[136] Furthermore, the Act broadens the government's ability to conduct searches in secret.[137]

---

132. ANDRADE, *supra* note 1.

133. In 1968, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act (OCCSSA) in response to the dramatic increase in government surveillance during the 1960s. Evans, *supra* note 19, at 951-53. OCCSSA required a government attorney to grant authorization to law enforcement officials in order for them to intercept electronic communications, and for officials to gain authorization from the Attorney General in order to intercept wire or oral communications. *Id*. at 953. Tracking devices, however, are explicitly excluded from the definition of "electronic communications." 18 U.S.C. § 2510(12)(C) (2000).

134. Pub. L. No. 107-56, 115 Stat. 272 (2001). Both houses of Congress passed the USA PATRIOT Act in fewer than six weeks following the attacks of September 11, 2001. H. Peter Del Bianco, Jr., *Is Big Brother Watching Out For Us?: The Case for Civil Liberties*, 17 ME. B.J. 20, 21 (2002). The Act passed with overwhelming support and almost no debate, as Senator Russ Feingold (D-WI) was the only voice of opposition in the Senate. *Id.* at 21, 28 n.2.

135. Michael T. McCarthy, Recent Development, *USA PATRIOT ACT*, 39 HARV. J. ON LEGIS. 435 (2002).

136. Del Bianco, *supra* note 134, at 25. The Act did not reduce the right to carry personal firearms, however, because the Attorney General argued that there was no current legal authority to make such a restriction. Marc Rotenberg, *Privacy and Secrecy After September 11,* 86 MINN. L. REV. 1115, 1119 (2002). The Attorney General failed, however, to make a similar argument regarding the right to obtain business information. *Id.*

137. Stanley & Steinhardt, *supra* note 17, at 9-10 (explaining that under the Act, U.S. intelligence could conduct a search of a citizen's home in secret, use evidence found to declare

II. ANALYSIS

A. Media Manipulation?

The fact that the media's increased reporting on child abductions has helped to create a market for personal tracking devices is undeniable,[138] but whether there was any *intention* to do so is left to speculation. Nevertheless, it is worth exploring why the possibility for intentional news manipulation may exist.

Because Americans get their information about current events from the media, news sources have become an authority on what is significant or trivial, true or false.[139] The corporate owners act as "gatekeepers" to information,[140] and critics believe that the mainstream media has the power to form public opinion by deciding what events to report and what meaning to ascribe to the events.[141] Because the corporate owners are so large and have ties that expand through political, social, and economic spheres; and as the lines between these spheres become increasingly blurred, the potential for news manipulation and subservience to these interests is enormous.[142]

---

the citizen an "enemy combatant," and imprison him without a trial).

138. *See supra* notes 58-67.

139. BAGDIKIAN, *supra* note 67, at xiiv.

140. EDWARD S. HERMAN, BEYOND HYPOCRISY: DECODING THE NEWS IN AN AGE OF PROPAGANDA 12 (1992).

141. NOAM CHOMSKY, NECESSARY ILLUSIONS 9 (1989). Chomsky describes in detail what he terms the "propaganda model," where discussion and debate are not outright restricted, but are instead fit within a framework that is suitable to state interest. *Id*. at 8.

142. *See* Jim Parker, *The CBS-Viacom Merger: Impact on Journalism*, 52 FED. COMM. L.J. 519, 522-25 (2000). One commentator poses the question:

> Is it a good idea for Time-Warner Chairman Gerald Levin to control the WB Network, HBO, TNT, TBS, CNN, CNNfn, CNNsi, Cinemax, Warner Bros., New Line Cinema, Hanna-Barbera, Castle Rock, Time, People, Sports Illustrated, Fortune, 28 other magazines, Warner Books, Little Brown, Warner Bros. Records, Atlantic, Elektra, Sire, Rhino, Time Warner Cable, and much more?

Simon, *supra* note 51, at 264 n.176. For a listing of holdings of the major media companies, see The Columbia Journalism review, at http://www.cjr.org/owners (last visited Nov. 2, 2003).

Arguing for heightened scrutiny by antitrust agencies and the FCC, late Senator Paul Wellstone asked: "As these far-flung multinational corporations extend their holdings and influence into more and more other industries, how much confidence can we have that they will hold any of those interests accountable to the people?" Wellstone, *supra* note 52, at 552. In news media, friends of the media, including major advertisers, are known as "sacred cows" because they are resistant to criticism. BAGDIKIAN, *supra* note 67, at 47. In one example, NBC

In short, as Noam Chomsky explains, major media (i.e., the elite media that establishes an agenda for the others to follow) are corporations engaged in "selling" an audience.[143]

For the many parents who felt vulnerable to kidnappings in recent years, seemingly the personal locator has emerged as a seemingly beneficial safety device.[144] The makers of these devices have seized the opportunity to use the media hype of abductions as a selling point for the locators.[145] Obviously, the many news items about personal locators do not discuss the relationship between the recent media attention towards child abductions and the timely release of the various personal locators, beyond it being a coincidence.[146]

Ultimately, the question of whether there is any connection between the media's reporting on child abductions and the release of the tracking devices is one of speculation. Even still, the close connection between mass media and corporate and state interests may have fueled the sudden media hype of child abductions. As such, one possible explanation is that the proprietors of these devices influenced major media to create a market for their products when they debuted in the marketplace. Given the capability of implants and tracking devices to implement surveillance in the most intrusive manner, others might be inclined to argue that the "conspiracy" extends a step further as part of a nationwide plan to implement "Big

---

asked Coca-Cola to review a documentary on Coca-Cola's use of migrant farmworkers before it aired. JOHNSTON, *supra* note 55, at 139. NBC removed segments of the documentary per Coca-Cola's request. *Id.*

143. CHOMSKY, *supra* note 141, at 8.

144. The numbers of news items that link the Summer 2002 child abduction case with parents' interest in personal locators are almost countless. *See, e.g.*, Kinnersley, *supra* note 14.

145. Apparently using guilt as a persuasive technique, an ADS spokesperson says, "[w]e have GPS units for our cars. If your car is stolen, we can locate it. Do we love our cars more than our children?" Kadaba, *supra* note 37 (quoting ADS Spokesman Matthew Cossollotto).

146. *See, e.g.*, Elliot Spagat, *Global Positioning Systems Are Now in Kids' Watches, Golf Toys, Even Fish Trackers*, WALL ST. J., Sept. 11, 2002, at D2 ("With growing concerns about child safety following a spate of abductions around the country, Wherify's timing is good.").

However, several reports do mention that Personal Locators had been in development for years *before* the media coverage and that the makers of these devices do not want to come across as capitalizing on kidnappings. Kathryn Balint, *GPS Kid: Satellite Locators Track Youngsters, but Practicality vs. Paranoia Debated*, SAN DIEGO UNION-TRIB., Dec. 16, 2002, at E1.

Brother,"[147] especially in light of post-September 11th measures to increase government surveillance.

B. The Shortfall of Current Privacy Law

The current safeguards against unwanted intrusions of privacy offer insufficient protection from novel technology like the personal locator. For one, the law of torts falls short of providing adequate protection of privacy. An individual wearing a device would most likely have no cause of action under the publicity tort, so long as the information is collected in public areas.[148] As such, one can create an extensive profile on an individual based on information collected from public areas.[149]

The intentional intrusion-of-privacy tort also offers little to protect privacy. Because the intentional intrusion of privacy tort is determined or limited by a reasonable expectation of privacy,[150] the fact that an individual uses a personal locator voluntarily naturally implies that she expects to forgo some of her privacy. This assumption, however, is problematic. Simply because she consents to use a personal locator does not per se imply that she expects or consents for the personal locator service provider to share the information with third parties.[151] Nevertheless, so long as the

147. One author, David Icke, envisions a "microchipped population" in which the population's every movement is monitored. DAVID ICKE, . . . AND THE TRUTH SHALL SET YOU FREE, 437-38 (1995). Years ago, he wrote: "The only thing that remains [in implementing this scheme] is persuading public opinion to accept it, or even demand it. One way this will be done is to highlight missing children stories, including abductions of babies from maternity wards." *Id.*

148. RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (1977).

Because personal tracking devices can track individuals regardless of whether they are in public or in private (notwithstanding the ability for the user to turn "off" the device, if available), if the individual is in a private location, such as his own home, he may have a cause of action under this tort if the private information were made public. *See id.* For example, if the individual was having an extra-marital affair, and if someone with access to the GPS data shared this information to a third party and then disclosed this matter, which would likely be offensive to a reasonable person, it would be grounds for a cause of action under this tort. *Id.*

149. *See supra* notes 71-73 and accompanying text.

150. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

151. *See* Balough, *supra* note 77, at 30. In discussing the use of GPS technology in rental cars, Balough explains that a renter who turns on GPS may not be giving sufficient consent for the rental company to share the data. *Id.* Balough cites to *Ainsworth v. Century Supply Company*, 693 N.E.2d 510 (Ill. App. Ct. 1998), which held that a plaintiff who gave consent to

individual is in a public place, it is unlikely that she can maintain an argument that there was a "reasonable expectation of privacy."[152]

One optimistic note for the future of protecting data from personal tracking devices lies in the FCC's approach to regulating cellular phone location information. If FCC regulations do indeed regard location information as a special class of CPNI, which specifically requires "opt-in" customer consent, then one can expect a similar willingness to protect the dissemination of location information from personal tracking devices.[153] However, the FCC regulations apply only to telecommunications carriers, and it is unclear whether personal locators will ultimately fall under the FCC's domain.[154]

C. The "Reasonable Expectation of Privacy" Test Is Ineffective Against Government Data Collection and Surveillance

Personal tracking devices will potentially present a significant threat to privacy with regard to government abuse in data collection and surveillance. With new technology such as the personal locator developing at a more rapid rate than that with which the law can keep pace, the potential for abuse intensifies.[155] More importantly, the bigger threat, as identified by Jay Stanley and Barry Steinhardt of the ACLU, is the "Synergies of Surveillance": the capability of the government to unify different technologies and data resulting in comprehensive surveillance and collection of data systems.[156] The

---

being videotaped when installing ceramic tile for an instructional video was not consenting to the video being aired on television. *Id.*

152. *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977).

153. Because the FCC refused to make a specific ruling on cellular phone location information, it is not entirely clear that "opt-in" consent is required. *See supra* note 99.

154. *See supra* note 101 (describing an e-mail to the author from an FCC representative expressing uncertainty over whether the FCC can regulate personal locators).

155. The personal locator is just one of many new devices that threatens privacy. Stanley & Steinhardt, *supra* note 17, at 16. Other devices include face recognition technology, the proposed national ID card, and the latest technology, "brain fingerprinting," which can supposedly read a persons thought patterns. *Id.* at 12-13.

156. *Id.* at 11-14. The authors propose the following illustration:

> A tourist walking through an unfamiliar city happens upon a sex shop. She stops to gaze at several curious items in the store's window before moving along. Unbeknownst to her, the store has set up the newly available "Customer Identification System," which detects a signal being emitted by a computer chip in her driver's license and records her identity and the date, time, and duration of her brief look inside

result of this comprehensive network could have an unprecedented chilling effect on society.[157]

In light of the United State Supreme Court's decision in *United States v. Knotts*,[158] and the Washington State Court of Appeals's examination of GPS devices in *State v. Jackson*,[159] a court seems likely to consider the wearers of personal locators *not* to have a reasonable expectation of privacy when they are in the public eye and have voluntarily worn the locator.[160] Therefore, under the current framework for analyzing the Fourth Amendment, it is unlikely that a court would grant protection from an unreasonable search should law enforcement access an individual's GPS location information even with a search warrant.[161] Similarly, because the Supreme Court's decision in *United States v. Kyllo*[162] involved an intrusion upon the home, the decision offers little in the way of protecting the location information of an individual who wears a personal locator from unwanted surveillance.[163]

Under the current judicial framework, Fourth Amendment protection is scarcely available when an individual is in a public

---

the window. A week later, she gets a solicitation in the mail mentioning her "visit" and embarrassing her in front of her family.

Id. at 1.

157. If individuals live with an awareness that they are under surveillance, then they will continually evaluate each decision they make, asking questions such as: "Will this make me look suspicious?" and "Will this reduce my ability to get insurance?" *Id*. at 14.

158. 460 U.S. 276 (1983).

159. 46 P.3d 257 (Wash. Ct. App. 2002).

160. *See supra* note 115 and accompanying text (discussing the holding in *Knotts*); *see also supra* text accompanying notes 115-24 (discussing the holding in *Jackson*).

161. The Supreme Court, in *Katz*, noted, "The Fourth Amendment protects people, not places," and therefore what an individual seeks to keep private, even if available to the public, could be protected. Katz v. United States, 389 U.S. 347, 351 (1967). Nevertheless, an individual voluntarily wearing a personal locator in public will find it difficult to argue that he expected privacy. *See supra* notes 150-52 and accompanying text.

162. 533 U.S. 27 (2001).

163. Once again, it would be difficult to argue that an individual who voluntarily wears such a device has an expectation of privacy when in public.

Despite the Court's reliance on the private location of the search in their decision, the ACLU considers the *Kyllo* decision to be an important step in protection of privacy from technology. Stanley & Steinhardt, *supra* note 17, at 17. The ACLU reasons that the Court's examination of the actual capabilities of thermal imaging devices demonstrates a willingness to reconsider the Fourth Amendment as applied to new technology. *Id.*

area.[164] Yet, new technologies that the framers of the Constitution could not have imagined, such as the personal locator, have the capability to conduct extensive searches through observation in public areas.[165] The current analysis amounts to a green light for the government to spy on individuals anytime they step outside of their homes.[166] Such an analysis is problematic in light of location-detecting technology. The arrival of E-911 in cell phones creates a system capable of tracking the always-increasing cell phone-carrying population whenever their phones are turned on.[167] Likewise, if an individual voluntarily wears a personal tracking device, he might also be opening himself to surveillance.

The current Fourth Amendment "reasonable expectation of privacy" standard is inadequate because the standard itself is defined by capability and pervasiveness of new technology.[168] As Professor Anthony Amsterdam observed thirty years ago, "the government could diminish each person's subjective expectation of privacy merely by announcing half-hourly on television . . . that we were all forthwith being placed under comprehensive electronic surveillance."[169] In other words, if the government announced flatly that they would conduct such surveillance, then it would no longer be subjectively reasonable to expect privacy. Likewise, once society accepts and integrates a technology, then it may no longer be reasonable to expect privacy from it.[170] If personal tracking devices

164. *See supra* note 115 and accompanying text.

165. Stanley & Steinhardt, *supra* note 17, at 16.

166. *See id.* at 16-17.

167. Hoofnagle, *supra* note 92, at n.83 and accompanying text. Although cellular telephone companies explain that bandwidth limitations only allow location tracking to occur when an individual receives or makes a call, Hoofnagle explains that companies foreseeably can increase bandwidth capacity, making constant tracking a realistic possibility. *Id.*

168. Ric Simmons, *From* Katz *to* Kyllo: *A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, at 1331-35 (2002) (quoting *Kyllo*, 533 U.S. at 34). *See also* Stanley & Steinhardt, *supra* note 17, at 16-17 (arguing that the reasonable expectation of privacy should not be defined by the capabilities of technology).

169. S. Bryan Lawrence III, Comment, *Curtilage or Open Fields?* Oliver v. United States *Gives Renewed Significance to the Concept of Curtilage in Fourth Amendment Analysis*, 46 U. PITT. L. REV. 795, 807 n.87 (1985) (quoting Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974)).

170. Simmons, *supra* note 168, at 1332. This conclusion is alluded to by the majority opinion in *Kyllo*, explaining that the use of intrusive technology might be a search if it is not "in general public use." *Kyllo*, 533 U.S. at 34. As the dissent explains, the threat to privacy actually

become widespread, then courts may not consider it reasonable to expect the GPS location information to remain private from government monitoring.

Acts of Congress offer users of personal locators little protection from government surveillance. Instead of strengthening privacy laws to meet new technology, acts such as the USA PATRIOT Act increase the government's ability to conduct surveillance and obtain information.[171] For example, the Act reduces the required standard of criteria to obtain information maintained by a business.[172] If the business is a personal-locator proprietor and the information is an individual's travel history or GPS data, the FBI could gain access to this data under the low relevance standard.[173]

III. PROPOSAL

The most immediate method for users of personal tracking devices to prevent proprietors from distributing consumer information is to secure privacy agreements with the companies. It is important for consumers to recognize the tremendous capability of these devices to intrude upon privacy, and for them to take active steps to protect their privacy and to make sure that the companies use the data only for its intended security purpose.[174]

Legislatures also need to take an active role in addressing the risk to privacy that new technologies, like the personal tracking device, present. One good start occurred in California, where the legislature introduced a bill containing a new invasion-of-privacy tort.[175] This privacy provision, which was ultimately defeated, required any company to obtain an individual's express permission before

---

increases if the technology is more widespread. *Id.* at 47 (Stevens, J., dissenting).

171. Stanley & Steinhardt, *supra* note 17, at 1, 9-10.

172. *See supra* note 136 and accompanying text.

173. *See* Del Bianco, *supra* note 134, at 25.

174. If the individual secures a privacy agreement and the proprietor breaches the agreement, then this could be a cause of action under the intentional intrusion tort. *See supra* notes 80-82 and accompanying text. The agreement would help to satisfy the difficult evidentiary burden of demonstrating a "reasonable expectation of privacy" while in the public eye, as the expectation comes from the agreement. *See supra* note 82 and accompanying text.

175. Renenger, *supra* note 2, at 564 (citing S.129 § 1798.100, 1999-2000 Reg. Sess. (Cal. 1999) (as amended Aug. 26, 1999)).

releasing his information to third parties.[176] Such an "opt-in" requirement is critical in protecting privacy.[177] If there is a presumption that information may be circulated unless otherwise expressed by the individual, the reality is that most individuals will not even be aware of the extent to which their personal information is gathered and distributed to the highest bidder. The United States Congress should adopt comprehensive privacy laws that protect all types of customer information.

Even more threatening than the commercial exploitation of this technology is the potential for governmental abuse. It is critical for Congress to enact comprehensive privacy laws protecting the public against surveillance.[178] While it is true that Congress must keep up with technological advances and evaluate the novel privacy concerns that they raise, technology will continue to progress at a rapid pace. A reactionary method of addressing privacy problems when they arise would be inadequate if each measure only addressed a specific kind of technology or information.[179] Congress should, therefore, adopt privacy laws that cut across different kinds of technology, including personal tracking devices.[180]

It would be highly unrealistic, however, to expect Congress to take such action when there is overwhelming support to weaken privacy laws.[181] Therefore, it is particularly important for the judicial system to address privacy issues within a new analytic frame. The best protection against unwanted surveillance is the Fourth Amendment's protection against unreasonable searches.

A necessary change in the courts' Fourth Amendment analysis is for the focus of "reasonable expectation of privacy" to move away

176. *Id.*

177. Polling data suggests that individuals prefer "opt-in" methods of obtaining consent to "opt-out" methods. Hoofnagle, *supra* note 92, at text accompanying nn.9-14, 48.

178. Stanley & Steinhardt, *supra* note 17, at 15.

179. The reactionary method by which Congress adopts privacy law has resulted in giving some interests strong privacy protection, while giving other similar interests weaker laws. *Id.* For example, strong privacy laws protect video store records as a response to Congressional disapproval over the release of Judge Robert Bork's video rental information during his bid for Supreme Court confirmation. *Id.* Yet, far weaker privacy laws protect other kinds of personal information, such as medical records or financial data. *Id.* The result is an inadequate patchwork set of privacy laws with far too many holes. *Id.*

180. *Id.*

181. *See supra* note 134 (discussing the rapid passage of the USA PATRIOT Act).

from the methods of search and surveillance, and instead to move towards the information itself.[182] As technology becomes more sophisticated, the questions of "how" and "where" the search is conducted should give way to the crucial question of "what" underlying information was gathered as a result of the search.[183] Whether an individual is in the public eye should not be given as much weight as it is currently given where advanced technology is concerned. The casual observer of a public event cannot come close to ascertaining the amount of data and analysis that a computer can. Each individual piece of new technology that threatens privacy is ultimately a component of a "Surveillance Monster" that can reach every facet of daily life.[184]

IV. CONCLUSION

Whether in the law of torts, federal privacy law, or the judiciary's Fourth Amendment analysis, current privacy law does not adequately protect the kind of privacy concerns raised by the personal tracking device. There must be significant safeguards to protect the personal, marketable data that a personal tracking device generates from circulation to interested third parties.

The personal tracking device creates a new realm of potential for government surveillance. Law enforcement could intercept an individual's GPS data, or access past information, making the individual constantly vulnerable to surveillance. Law enforcement's ability to do so is becoming more pervasive as recent legislation, such as the USA PATRIOT Act, loosens restrictions to accessing data when conducting an investigation.

---

182. Simmons, *supra* note 168, at 1321-24. By focusing on the method of surveillance, courts engage in the needlessly complex inquiry of drawing analogies, asking questions such as: "[I]s thermal imaging analogous to watching snow melt off a roof or is it more like using binoculars? Or perhaps it is most analogous to using a dog to detect the odor of illegal contraband?" *Id.* at 1332 (internal citations omitted).

183. *Id.* at 1324-27. Simmons poses the question, "[W]hen the government observes our backyard, do we really care if they are doing it undetectably and legally from a satellite miles in the air or blatantly and illegally from a helicopter hovering ten feet above us?" *Id*. at 1324. By overemphasizing the method of surveillance, courts set a dangerous precedent that surveillance is okay if it does not feel intrusive. *Id*. at 1327.

184. Stanley & Steinhardt, *supra* note 17, at 2, 14.

The most important step to protecting privacy is to increase public awareness of these issues. While personal tracking devices offer safety benefits, consumers should be aware of the significant privacy issues that these devices present. Further, the public must be aware of the bigger picture behind each new technology and each looser surveillance regulation: each bit of information can be collected and combined to form a comprehensive profile.[185] If the public allows a new intrusion on privacy without hesitation, then ultimately this will become accepted as a normal part of life.[186]

When the defendant in *United States v. Knotts* cautioned the Court against allowing twenty-four hour surveillance of any citizen, the Court replied that when that day comes, there will be enough time for the courts to reevaluate the relevant constitutional principles.[187] The *Knotts* Court misjudged the abundance of time available to reevaluate its Fourth Amendment analysis, as technology is developing at an increasingly rapid pace. It is urgent for the courts and the public to reevaluate privacy rights and related consumer expectations.

---

185. *Id.* at 2. Stanley and Steinhardt write:

> [U]nless each new development is also understood as just one piece of the larger surveillance mosaic that is rapidly being constructed around us, Americans are not likely to get excited about a given incremental loss of privacy like the tracking of cars through toll booths or the growing practice of tracking consumers' supermarket purchases.
>
> We are being confronted with fundamental choices about what sort of society we want to live in. But unless the terms of the debate are changed to focus on the forest instead of the trees, too many Americans will never even recognize the choice we face, and a decision against preserving privacy will be made by default.

Id. at 14-15.

186. *Id.*

187. *See supra* note 115 and accompanying text.